Research and application of EJBCA based on J2EE

Liyi Zhang[1], Qihua Liu[2] and Min Xu[3]
1 Center for Studies of Information Resources, Wuhan University,
430072, Wuhan, P.R.China
lyzhang@whu.edu.cn
2 Center for Studies of Information Resources, WuhanUniversity,
430072,Wuhan, P.R.China
qh_liu@163.com
3 Center for Studies of Information Resources, Wuhan University,
430072,Wuhan, P.R.China
xu19870107@yahoo.com.cn

Abstract. This article carries on the exhaustive analysis and the research of the opened source system EJBCA based on the J2EE, furthermore conducts the distribution and deployment in accordance with the required software on the Linux platform, on this basis, and builds a specific application example of EJBCA. In the end, the authors have carried on the prospect about expansion and practical application capacity of EJBCA system, hope to have the important significance of model to the independent own research and development of present domestic PKI technology and product.

1 Introduction

To ensure the confidentiality, authenticity, integrity and non-repudiation of online transmission of digital information, so that to ensure its security on the network transmission, in addition to use a stronger encryption algorithm in telecommunication transmission and other measures, it's necessary to establish a trust and verification mechanism. In other words, the parties who participate in e-commerce and e-government must have a logo that can be verified, which is the digital certificate.

Digital certificates are a proof of identity of some entities merchant/ enterprise, gateway/bank etc) in the on-line communication and the commercial transaction activity [1].It is unique, and takes together the public key of entities with the entities itself. To achieve this purpose, digital certificates must comply with the international standard of x.509 and have a reliable source. This means that we must have an authority, which is trusted by every entity in internet, responsible for the distribution and management of digital certificates, and

Please use the following format when citing this chapter:

Zhang, L., Liu, Q., Xu, M., 2007, in IFIP International Federation for Information Processing, Volume 251, Integration and Innovation Orient to E-Society Volume1, Wang, W. (Eds), (Boston: Springer), pp. 337-345.

ensures the security of online information, it is certificate authority. Its existence is the basis for the existence of e-commerce and e-government.

Now, well-known CA software are researched and developed by enterprises of foreign countries. To obtain a legal certificate from this authority, the first required is to pay the high costs of certification, the second, we don't master core technologies about the CA software, so it is inconvenience to implement the high-encrypted application, but the amount of the independent own research and development of present domestic CA software is few, and that this software all depend on the operating system platform, which using J2EE is minimal. So, it is the best way for some important government authorities、enterprises and education department to build their own certificate authority. The OSFS of Linux and open-source project based on java provide an unprecedented opportunity for our own research on CA software. This article carries on the exhaustive analysis and the research of the famous opened source system EJBCA based on the internet of sourceforge.net, furthermore conducts the distribution and deployment in accordance with the required software on the Linux platform, on this basis, and builds a specific application of EJBCA. In the end, the authors have carried on the prospect about expansion and practical application capacity of EJBCA system, hope to have the important significance of model to the independent own research and development of present domestic PKI technology and product.

2 The basic framework of EJBCA

EJBCA is an enterprise class Certificate Authority using J2EE technology. EJBCA builds on the J2EE platform to create a robust, high performance, platform independent, flexible, and component based CA to be used standalone or integrated in any J2EE app [2].

J2EE——Java 2 Enterprise Edition, is an enterprise application solutions based on the java 2 platform.J2EE is not a product, but a range of criteria. Not only does it have all functions of the J2SE platform, but also provides the full support of EJB, Servlet, JSP,XML technology and etc, Its ultimate goal is to become an architecture of supporting for the enterprise-level application and development, simplify a series of complicated problems about the development、deployment and management of enterprise solutions.

J2EE uses multi-tier distributed application model. This model is divided into several functional components, which are distributed with different host machines according to different layers where they are located in. These layers include client layer、WEB tier、business tier and data tier [3]. Business tier is also named EJB tier in EJBCA, which contains two major components——RA component and CA component, system framework of EJBCA is shown in Fig.1.

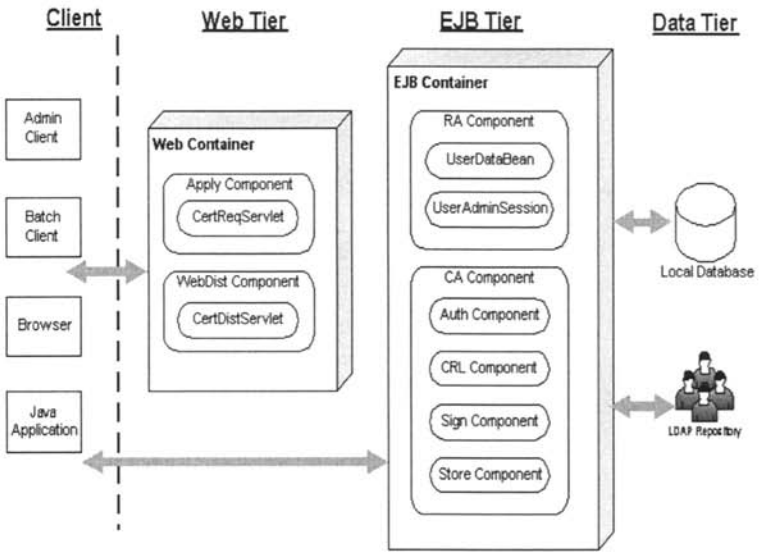

Fig. 1. System framework of EJBCA

2.1 The main components of EJBCA

Fig.1 shows that EJBCA system is mostly composed of Web component, RA component, CA component, LDAP server and database server [4].

(1) Web Component

It is mainly faced to ordinary users, and used to provide some request and services such as CertReqServlet, CertDistServlet, CertBroServlet and etc between the application server (RA component and CA component) and client browser. At the first, users receive certificates of Web component through application server. In the second, all communications between users and Web components, including some information of users and public key of browser, are encryption transmitted through encryption key of Web component. So, it is very safe to apply and transmit certificates, the process is shown in Fig. 2.

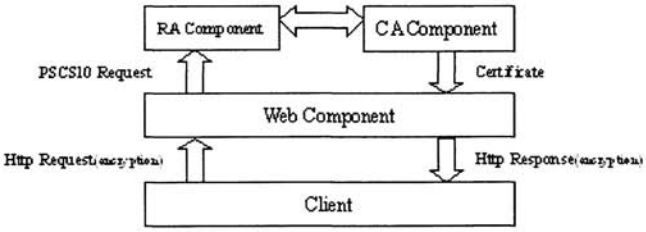

Fig. 2. The process of information transmission in EJBCA

(2) RA Component

It is also named registered authority, mostly provides some functions of user registration and auditing. RA component plays a bridging role in EJBCA. On the one hand, it transmits services of Web component's CertReqServlet and CertDistServlet to CA component; on the other hand, it transmits services of CRL and certificates which are given by CA component to LDAP and Web component.

(3) CA Component

It is the core component in EJBCA, can provide some functions such as CertDistServlet, certificate signature, certificate storage, CRL, SubCA foundation and etc. First, CA components have their own private key and public key, and then transmit certificates which are given by CA to RA component through Web component. CA also has responsibility to generate some digital certificates for all levels of administrations, such as Web components, subCA and RA. In EJBCA, types of certificate are optional. There are three types in the initialization time, ENDUSER (FIXED), ROOTCA (FIXED) and SUBCA (FIXED). In addition, users also can define their own types of certificates.

(4) LDAP Server

It provides service of catalog browsing, and charges for adding users' information and digital certificates which are transmitted by RA to servers. So, other users can receive their digital certificates through visiting LDAP server. In EJBCA, configurations of LDAP serve are optional; we can match certificates and their list to relevant LDAP servers through amending configuration files of LDAP [5].

(5) Database Server

It is a very important component in EJBCA, used to storage and manage users' information, digital certificates, diary document, statistical information and etc.

2.2 The construction of EJBCA

(1) Software installation and configuration environment variable

Download and install the relevant software Jdk 1.4.2, JBoss4.0.1 SP1, ejbca3.0.7, jce_policy-1_4_2 and apache-ant-1.6.3. System database can choose from among SqlServer, Mysql, Oracle, and etc, we use Mysql in this article. It is necessary to configure environment variables after configuring relevant software. There are several environmental variables which must be allocated: Jdk, Ant and Jboss. First, use sentences of "export" to assignment categories of Jboss, Jdk and Ant to variables of JBOSS_HOME, JAVA_HOME and ANT_HOME in the operation system of .Linux. Second, add these sentences to the tail of the document of "/etc/profile", which locate in the installation directory of EJBCA.

(2) The deployment of EJBCA

Implement the command of "ant" to compile EJBCA source code in the directory of EJBCA. The internal business logic and deployment descriptor of CA will be packaged into an enterprise application file of "ejbca-ca.ear" after running the command of "#ant deploy". Copy this file to the deployment directory of Jboss. So far, the entire CA system of EJBCA has been deployed to server of Jboss. Use sentences of "CREATE" to grant the database of Mysql. But, it is necessary to establish an own certificate authority before running the EJBCA, this is root CA. And, it must be established on the J2EE sever. First, start the server of Jboss. Second, implement the command of "#install.sh" in the

directory of "EJBCA". In the installation process, CA will create three types of certificates: client administration certificate, sever certificate and certificate which is signed by root CA. Client administration certificate and server certificate locate in the directory of "P12", which is subdirectory of EJBCA directory, but the certificate of root CA locate in the letter. On the one hand, the certificate of root CA is automatically imported into the private key file of "carcerts" which locate in the Jdk security directory of "JAVA_HOME\lib\security", "JAVA_HOME" is installation directory of Jdk. On the other hand, the server certificate is imported into directory of "JBOSS_HOME\bin"; "JBOSS_HOME" is installation of Jboss. Ii is necessary for EJBCA to manage CA in SSL layer, so client needs to import the client certificate of "P12/superadmin.P12" into browsers, and then can manage CA through browsers.

(3) The configuration of Two-way SSL

The SSL protocol is a standard protocol to ensure the secure communication between the Web browser and Web server, which is developed by Netscape. It is located in the transport layer. It is seen as a standard security measure of server and web browser. The methods of configuration of EJBCA are as follows:

First, open the browser; input the address of http://localhost:8443/ejbca/adminweb; obtain the certificate of root CA. Second, add users of client and server in home page; designate the method of building private key. Third, input user names and password of client and server preserve the file of ".req" and install these certificates through the installation guide. A point worth noting is that we must award certificates to every client who can visit server and server through using root CA in the process of configuration of Two-way SSl.

3 The example of EJBCA application

In this article, authors design a demonstration example of EJBCA application, and use some specific figures of framework to display the building process of a small certificate authority. Through description of the example, authors conduct a detailed analysis of how to use the famous system EJBCA for practical application, and make it productive.

3.1 The introduction of EJBCA application example

The application example of PKI/CA is a small certificate system, which has two root CAs. One is certificate authority of china education (China IC). Its responsibility is to provide certification for a number of entities in the field of education. For example, school can certificate candidates' information in graduate entrance examination. It is not necessary to check manually students' identity. Conversely, students also can see authentication information of schools in order to avoid being taken. Another is certificate authority of Wuhan logistics (WHU ECLAB). Its main objective is to certificate entities of china special transport network, such as vehicles, drives, maintenance units. The basic framework of the application example is shown in Fig.3.

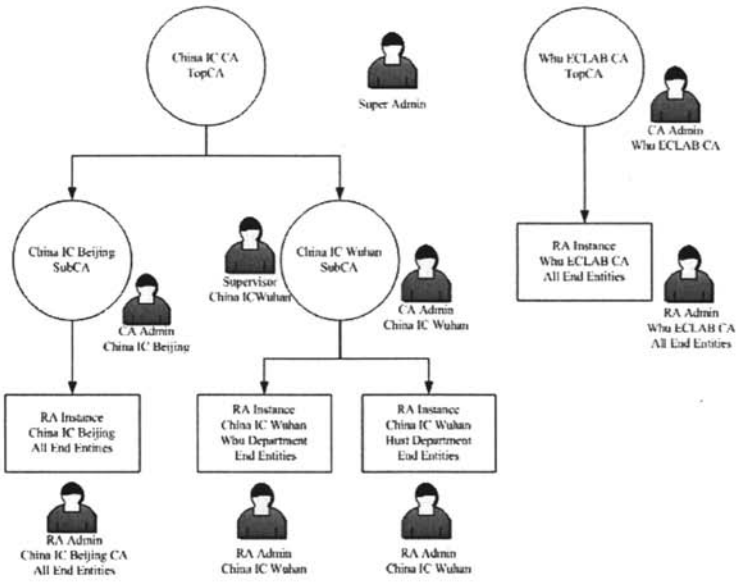

Fig. 3. The basic framework of the application

Note: In this figure, circular used to show examples of CA, rectangular used to show examples of RA

Can be seen from the Fig.3, the application example has the following characteristics:

（1）The certificate authority consists of two separate bodies, each one has a root CA.

（2）Whu ECLAB is a simple PKI, and only has a CA and a RA.

（3）China IC has two branches in Beijing and Wuhan. Therefore, each branch has a subCA; in particular, the branch of Wuhan all has businesses in the two schools of WHU and HUST.

（4）China IC education need three examples of RA to manage.

3.2 The building of EJBCA application example

We will build the system of PKI/CA from the perspective of roles. The system is divided into four roles, and is shown in Fig.4.

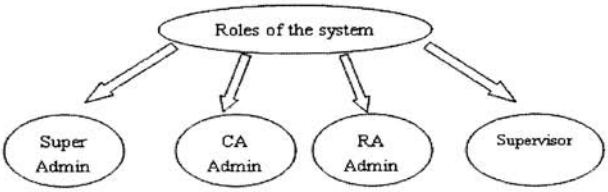

Fig. 4. Roles of the application

(1) Super Admin

He has the authority to manage the entire system. As the role of super admin, he can do some things, such as editing system configuration, managing CA, building CA admin and etc. Detailed below:

①System configuration. Set up the title, slogans and language of the top and tail of pages, the theme and the number of data of each page. Choose the item of "Enable End Entity Profile Limitations" to manage RA, and set up two items of "Enable Key Recovery" and "Issue Hardware Tokens" to "unchecked".

②Manage publisher. The publisher connects some form of certificate storage system, whose certificates will be sent to the entity. A publisher is a LDAP directory or Active directory or publisher connector of definition established. We will build two publishers:

A、China IC LDAP
suffix "O=China IC,C=CN"
rootdn "CN=Manager,O=China IC,C=CN"

B、WHU Eclab LDAP
suffix "O=WHU Eclab,C=CN"
rootdn "CN=Manager, O= WHU Eclab, C=CN"

③Manage CAs. Now we need to build the structure of CA. Can be seen from Fig.4, root CA of China IC will have two subCAs. One is China IC Beijing, another is China IC Wuhan. But WHU Eclab only has a root CA, it is Whu ECLAB CA. We designate that every CA all has a private key of RSA. Its length is 2,048 spaces, and it also can be valid for 10 years.

④Establish CA admin. In the PKI system, we allow the companies to manage their own certificates and RAs. We hope to have a major admin in each place. "China IC Beijing CA Admin" and "China IC Wuhan CA Admin" are administrations of China IC in Beijing and Wuhan. But "Whu Eclab in China" is an administration of Whu ECLAB in china. It is crucial that the administrators should not see each other's data, such as users, log, and etc, especially when two agencies are competitors.

(2) CA Admin

His responsibilities include managing certificate files and terminal entity files, configuring log and establishing RA admin.

(3) RA Admin

He is responsible for establishing/compiling/canceling/deleting terminal entity and seeing existent entities and their historical record. An RA only can manage the terminal entity of their own purview, so each other are transparency, as shown in Fig.5.

Fig. 5. The relation of RAs

(4) Supervisor

His responsibility is seeing entities and visiting logs.

4 Prospect

To conclude this article, the authors also consider the expansion and application capability of EJBCA. EJBCA system can be found through studying that it will have further expansion in the following areas.

(1) The improvements of encryption algorithm

EJBCA is a component –based structure. Users can develop or introduce some secret encryption algorithms to embed in EJBCA. And they also can develop their certificates and this certificates' list in accordance with the agreement of X509.

(2)The expansion of web registration mechanism

Client entities of the system are added by RA admin in the background. In fact, we can examine and certificate information through web registration mechanism when the number of users is very large [6, 7].

(3) Use technology of hardware and fingerprint recognition to certificate entities' identity

Users can use certain hardware (such as a simple encryption card) to communicate with procedures to verify identity. They also can design an identification system based on the characteristics of the fingerprint, and add this system to EJBCA as a component.

(4)The transplantation of EJBCA

EJBCA is developed on the basis of application sever of Jboss. But now a large number of enterprises and organizations all use other servers, such as IBM Websphere, BEA Weblogic and etc. So, the transplantation is a problem worth studying. The authors have utilized BEA Weblogic server to configure EJBCA, and proved its feasibility.

In summary, EJBCA is assembly simple, flexible, easy to manage. It can be applied to the security framework of e-government and e- commerce through transplantation and appropriate allocation. EJBCA is a valuable opened source system, has the important significance of model to the independent own research and development of present domestic PKI technology and product.

References

1. Z.S. Guan, *Public key infrasture and certificate authority*, Publishing House of Electronics Industry, Beijing (2002).

2. Ejbca-design. http://sourceforge.net/project/showfiles.php?group_id=39716.

3. R. Johnson and H.P. Wei , *The guile of J2EE design and development*, Publishing House of Electronics Industry, America (2003).

4. EJBCA: readm.txt.http://ejbca.sourceforge.net/do-cs/frame.htm.

5. Q. Chen and Q.S. Ling, The example of security CA——research of EJBCA, *Computer Engineering and Design* (2005).

6. X. Chen, The design and development of EJBCA, Wuhan:Wuhan University, 2006.

7. H. Zhang, Research on the Security Authentication of Electronic Commerce and the Design and Implementation of the CA Model, *Computer technology* (2006).

8. B.S. Zhou and L. Zhang, Research of EJBCA on WPKI environment, *Computer Engineering and Design* (2005).

9. T.W. Xiao,S.Y. Zhang and Y.P. Zhong, Design and Implementation of PKI/CA-based Middleware System, *Computer Engineering* (2006).

10. J.C. Li and H.L. Liu, Research on Secure Payment Protocols of Electronic Commerce, *Value Engineering* (2006).

11. L.N. Lan and X.Y. Liu, Research on Security Architecture in E-Commerce System, *China Information Security* (2007).

12. Q.H. Shuai, The Analysis of safe Certificate in E-Commerce, *Net Security Technologies and Application* (2007).

13. PKI Tutorial. http://www.cs.auckland.ac.nz/pgut001/pubs/pkitutorial.pdf.

14. EJBCA-Architecture. http://sourceforge.net/project/showfiles.php?group_id=3971.

15. Enterprise Text Message Platform. http://www.jrsoft. com.cn/Product/Aviation/sm s. asp.[2007-03-20].